

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号
特表2003-513349
(P2003-513349A)

(43) 公表日 平成15年4月8日(2003.4.8)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 15/00	3 1 0	G 0 6 F 15/00	3 1 0 P 5 B 0 8 5
	3 3 0		3 3 0 A

審査請求 未請求 予備審査請求 有 (全 37 頁)

(21) 出願番号 特願2001-533487(P2001-533487)
(86) (22) 出願日 平成12年10月25日(2000.10.25)
(85) 翻訳文提出日 平成14年4月25日(2002.4.25)
(86) 国際出願番号 P C T / I L 0 0 / 0 0 6 7 7
(87) 国際公開番号 W O 0 1 / 0 3 1 4 1 5
(87) 国際公開日 平成13年5月3日(2001.5.3)
(31) 優先権主張番号 6 0 / 1 6 1 , 4 7 3
(32) 優先日 平成11年10月25日(1999.10.25)
(33) 優先権主張国 米国 (U S)

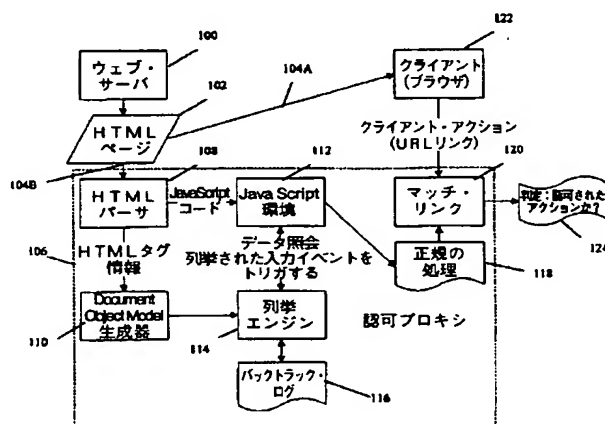
(71) 出願人 サンクタム、リミテッド
イスラエル国、ヘルズリヤ、サビア ストリート 1、ビー、オー、ボックス 12047
(72) 発明者 モラン、タル
イスラエル国 テル アビブ、ホフェイン ストリート 10
(72) 発明者 エル - ハナニ、ユヴァル
イスラエル国 テル アビブ、ラサル ストリート 10
(74) 代理人 弁理士 浅村 皓 (外3名)

最終頁に続く

(54) 【発明の名称】 クライアントの要求を確認する方法およびシステム

(57) 【要約】

クライアントとデータ処理システムのサーバとの間で送信された要求されたアクションの実行を認可するシステムおよび方法が提示されている。該方法は、アクションのセットを含んでいるメッセージを受信し、そのアクションのセットの実行をシミュレーションすることを含む。許容可能なアクションと、シミュレーションしたアクションへのユーザが定義可能な入力とを表すリストが定義される。次いで、許容可能なアクションと、許容可能なアクションへのユーザが定義可能な入力は、ユーザが要求したアクションおよび入力と比較される。ユーザが要求したアクションおよび入力内の要素が、許容可能なアクションと入力のリストに含まれているとき、ユーザが要求したアクションおよび入力は、実行を認可される。



【特許請求の範囲】

【請求項1】 クライアントとデータ処理システムのサーバとの間で送信された要求されたアクションの実行を認可する方法であって、

アクションのセットを含んでいる第1メッセージと、ユーザが要求したアクションおよび入力を含んでいる第2メッセージを受信することと、

アクションのセットの実行をシミュレーションし、許容可能なアクションと許容可能なアクションへのユーザが定義可能な入力とのリストとを構築することと、

許容可能なアクションとユーザが定義可能な入力とのリストを、ユーザが要求したアクションおよび入力と比較することとを備え、

許容可能なアクションとユーザが定義可能な入力とのリストが、ユーザが要求したアクションおよび入力を含み、ユーザが要求したアクションの実行を認可する方法。

【請求項2】 シミュレーションのステップが、クライアントにおけるアクションのセットの実行から得られるすべての可能なアクションと、可能なアクションへの入力とを識別することを備える、請求項1に記載の方法。

【請求項3】 シミュレーションのステップが、アクションのセット内にある各コマンド、フィールド、ユーザが選択可能な入力オプション、およびHTTP要求を呼び出し、およびトリガすることを備える、請求項1に記載の方法。

【請求項4】 ユーザが要求したアクションおよび入力が、クライアントにおける第1メッセージの受信に応答して実施されたユーザ・セッション中に提供されたアクションと入力とを含む、請求項1に記載の方法。

【請求項5】 シミュレーションのステップ中に、データ値のエントリを要求する入力制御を検出し、そのデータ値を表すために、固有の配置ホルダを割り当てることと、

比較のステップ中に、固有の配置ホルダのパターンを、ユーザから受信した入力に整合させることとを備える、請求項1に記載の方法。

【請求項6】 シミュレーションのステップが、

複数の事前に定義されたデータ値の1つを選択することを要求する入力制御を

検出することと、

複数の事前に定義されたデータ値の各々が選択され、かつリストされるまで、複数の事前に定義されたデータ値1つを対話式に選択し、アクションのセットのシミュレーションを続行し、選択された1つのデータ値を有する許容可能なアクションとユーザが定義可能な入力とのリストを構築することとを備える、請求項1に記載の方法。

【請求項7】 シミュレーションのステップの前に、クライアントにおいてアクションのセットの実行を追跡することと、

シミュレーションのステップ中に、ユーザが選択可能な入力に応答して、追跡の結果を提供することとを備える、請求項1に記載の方法。

【請求項8】 シミュレーションのステップの前に、

第1メッセージのアクションのセット内にあるアクションを識別することと、識別されたアクションへの入力を追跡するために、アクションで第1メッセージを補足することと、

補足された第1メッセージをクライアントに送信することと、

シミュレーションのステップ中に、識別されたアクションへのユーザが選択可能な入力が要求された際に、追跡の結果を提供することとを備える、請求項1に記載の方法。

【請求項9】 追跡の結果が、第2メッセージ内に含まれている、請求項8に記載の方法。

【請求項10】 追跡の結果が、第2メッセージを受信する前に受信された第3メッセージに含まれている、請求項8に記載の方法。

【請求項11】 クライアントとデータ処理システムのサーバとの間で結合されたセキュリティ・ゲートウェイであって、

前記クライアントとサーバとの間の送信を評価し、かつ、各送信内に含まれている情報内容とアプリケーション・プログラミング論理を識別するための評価装置と、

前記送信の前記アプリケーション・プログラミング論理を実行する処理環境をシミュレーションするシミュレータであって、事象をトリガし、かつ、前記アプ

リケーション・プログラミング論理へのユーザが定義可能な入力を識別するための列挙エンジンを含み、許容可能なアクションと、前記アクションへのユーザが定義可能な入力値とのリストを提供するシミュレータと、

ユーザが要求したアクションおよび入力を含んでいる送信を受信し、前記ユーザが要求したアクションおよび入力を、前記許容可能なアクションとユーザが定義可能な入力値とのリストと比較し、前記許容可能なアクションと入力値とのリスト内にあるユーザが要求したアクションおよび入力を有する送信を前記セキュリティ・ゲートウェイを通して渡すフィルタとを備える、セキュリティ・ゲートウェイ。

【請求項12】 前記許容可能なアクションと入力値とのリストを記憶するために、前記シミュレータと前記フィルタによってアクセス可能なデータ・ストアを備える、請求項11に記載のセキュリティ・ゲートウェイ。

【請求項13】 前記シミュレータが、データ値のエントリを要求する入力制御を検出し、かつ、前記データ値を表すために、固有の配置ホルダを割り当てるための検出器を備え、前記フィルタが、前記固有の配置ホルダのパターンを、前記ユーザから受信した前記入力に整合させるための手段を備える、請求項11に記載のセキュリティ・ゲートウェイ。

【請求項14】 前記シミュレータが、

複数の事前に定義されたデータ値の1つを選択することを要求する入力制御を検出する検出器と、

前記複数の事前に定義されたデータ値の各々が選択され、かつリストされるまで、前記複数の事前に定義されたデータ値の1つを対話式に選択し、前記アプリケーション・プログラミング論理のシミュレーションを続行し、前記選択された1つのデータ値を有する許容可能なアクションとユーザが定義可能な入力とのリストを構築する手段とを備える、請求項11に記載のセキュリティ・ゲートウェイ。

【請求項15】 前記評価装置が、前記アプリケーション・プログラミング論理内において、関心のあるアクションを識別し、かつ、クライアントにおいて受信した前記アクションへの入力を追跡するための手段を備え、前記シミュレー

タが、前記追跡の結果を受信し、かつ、前記識別されたアクションへのユーザが定義可能な入力、前記シミュレーション内において実施される際に、前記追跡の結果を提供するための手段を備える、請求項11に記載のセキュリティ・ゲートウェイ。

【請求項16】 クライアントからクライアント/サーバ・データ処理システムに送信された要求されたアクションの実行を認可する方法であって、クライアントとサーバの間に結合されたゲートウェイによって実施され、

サーバから、アクションのセットを含んでいるドキュメントを受信することと

、
アクションのセットの実行をシミュレーションし、許容可能なアクションと、許容可能なアクションへのユーザの定義可能な入力とのリストを構築することと

、
クライアントから、ユーザが要求したアクションおよび入力を含んでいるメッセージを受信することと、

許容可能なアクションとユーザが定義可能な入力とのリストを、ユーザが要求したアクションおよび入力と比較することとを備え、

許容可能なアクションとユーザが定義可能な入力とのリストが、ユーザが要求したアクションおよび入力を含み、ユーザが要求したアクションおよび入力を、実行のためにサーバに送信する方法。

【請求項17】 ゲートウェイにおいて、許容可能なアクションとユーザが定義可能な入力とのリストを記憶することを備える、請求項16に記載の方法。

【発明の詳細な説明】

【0001】

(著作権の注意)

本出願ドキュメントの部分は、著作権保護を受ける内容を含む。著作権の所有者は、特許事務所または商標事務所の特許ファイルまたは記録にあるように、誰もが出願ドキュメントまたは出願の開示をファクシミリで再生することに異存はないが、そうでない場合、すべての著作権を保有する。

【0002】

(関連する出願)

本出願は、以下の同時係属中の出願に関連する。

- ・ 1999年10月25日に出願された、弁理士整理番号第3269/8号であるMETHOD AND SYSTEM FOR VERIFYING A CLIENT REQUESTという名称の米国仮特許出願第60/161, 473号

- ・ 1999年7月1日に出願された、弁理士整理番号第3269/6号であるMETHOD AND SYSTEM FOR EXTRACTING APPLICATION PROTOCOL CHARACTERISTICSという名称の米国特許出願番号第09/345, 920号

- ・ 1998年9月9日に出願された、弁理士整理番号第3269/3号であるMETHOD AND SYSTEM FOR PROTECTING OPERATIONS OF TRUSTED INTERNAL NETWORKSという名称の米国特許出願番号第09/149, 911号

- ・ 1998年9月9日に出願された、弁理士整理番号第3269/4号であるMETHOD AND SYSTEM FOR MAINTAINING RESTRICTED OPERATING ENVIRONMENTS FOR APPLICATION PROGRAMS OR OPERATING SYSTEMSという名称の米国特許出願番号第09/150, 112号

- ・ PCT出願PCT/IL98/3269/4

- ・ PCT出願PCT/IL98/00443

・PCT出願PCT/IL00/00378

これらの出願の開示は、参照することによって、完全に本明細書に組み込まれている。

【0003】

(発明の背景)

本発明は、一般に、プライバシーおよびセキュリティのシステムに関し、より詳細には、データ処理システム内において、クライアント装置とホスト装置との間で送信された要求、データ、情報内容、アプリケーション、および他の情報を認可する方法およびシステムに関する。

【0004】

(従来技術)

クライアント/サーバ・データ処理システムでは、いくつかのパーソナル・コンピュータ、ワーク・ステーション、携帯式および/または手持ち式装置など（「クライアント」）は、1つまたは複数のホスト・コンピュータ（「サーバ」）と連結され、かつ通信している。サーバは、ネットワーク上でクライアントによって共有されている情報および/またはアプリケーション・プログラムに対するクライアントからの要求を処理する。ますます、クライアント/サーバ・ネットワークは、例えば、それ自体がワールド・ワイド・ネットワークの一部である、すなわち、インターネットのワールド・ワイド・ウェブの一部（「ウェブ」）であることが可能であるイントラネットおよびエキストラネットなど、より広範な「ネットワークのネットワーク」を形成するために、連結されるようになってきた。ネットワークを連結することにより、クライアントは、ネットワークにわたって、リソース（例えば、情報およびアプリケーション・プログラム）を供給することが可能になる。

【0005】

潜在的にワールド・ワイド・ネットワーク上で、共有されている情報およびアプリケーション・プログラムの利用可能性が増大するにつれ、個々のクライアント/サーバ・ネットワークの各々の脆弱性が増大している。例えば、ネットワークの1つに記憶されている所有権を主張できる情報およびアプリケーション・プ

プログラムを検索および／または損傷しようとする不謹慎な個人は、所有権を主張できる情報およびアプリケーション・プログラムにアクセスして、無認可の方式で、それを使用する可能性がある。そのような無認可の使用を防止する努力では、多くのネットワークは、「ファイアウォール」を通して、他のネットワークに接続されている。従来のファイアウォールは、内部ネットワーク・リソース（例えば、特有のウェブ・サーバまたはフォルダ）へのアクセス制御に対処し、ネットワークの部分へのアクセスを制限し、および、それに記憶されている所有権を主張できる情報およびアプリケーション・プログラムに対する無認可の検索または損傷を防止するように設計されたハードウェアおよび／またはソフトウェア・システムを含む。

【0006】

しかし、多くの従来のファイアウォール・システムは、アプリケーション・レベルでは認可に対処せず、認可されたクライアントであると偽った不謹慎な個人によって機能しなくなる可能性がある。例えば、多くのウェブ・アプリケーションは、アプリケーションのユーザは、実際に彼／彼女のブラウザ上でアプリケーションのモバイル・エージェントを実行していると想定している。しかし、悪意のあるユーザは規格のウェブ・ブラウザ・ソフトウェアを使用せずにウェブ・サーバに接続することができ、したがって、そのユーザはブラウザ側で強化することが可能である制限になんら束縛されず、悪意のあるユーザは、標準的なクライアントであると偽って、ウェブ・サーバに破壊的なまたは捏造したデータを送信することができる。

【0007】

共通して譲受された米国特許出願第09／345,920号には、標準的なHTMLドキュメントのユーザからの要求を確認するための解決法が記載されている。その解決法は、HTMLドキュメントの内容（「認可されたアクション」）に基づいて、ブラウザ・ソフトウェアが取ることが可能であるアクションのセットまたはパターン（HTTP要求）を抽出することに基づいている。次いで、この認可されたアクションのセットは、クライアントのアプリケーションによって送信された要求に対して整合される。ユーザが、規格のブラウザの1つを使用し

ていない場合であっても、アクションの法的または認可されたセット内からの要求のみが、ウェブ・サーバに渡されることになる。

【0008】

以上の内容を考慮して、本発明の発明者は、上述した確認技術を、ウェブ・サーバの代わりにクライアント・システム上で実行する論理（例えば、HTMLページに埋め込まれたJavaScript（TM）プログラム）に拡張する必要性を認識した。特に、本発明者は、外部データとその上で起きている事象を入手および確認するために、クライアント・サイドの論理の実行をシミュレーションする必要性を認識した。

【0009】

（発明の簡単な概要）

本発明の目的は、サーバ・システムの代わりに、クライアント・システム上で実行する論理のための確認技術を提供することである。

【0010】

本発明の他の目的は、クライアント・サイドの論理（例えば、HTMLページに埋め込まれたJavaScriptプログラム）のための確認技術を提供することである。この技術は、外部データとそこで起きている事象を入手および確認するために、論理の実行をシミュレーションする。

【0011】

本発明のさらに他の目的は、外部データと事象とに対する認可された要求のみが、クライアントから保護されたサーバに渡されるように、論理の実行をシミュレーションするクライアント・サイドの論理のための確認技術を提供することである。

【0012】

本発明の他の目的および利点は、図面とそれに続く記載を考慮することから、より明らかになるであろう。

【0013】

以上および他の問題点は、克服され、目的は、システムおよび方法が、クライアントとデータ処理システムのサーバとの間で送信された要求されたアクション

の実行を認可するために提示されている、本発明の実施形態による方法および装置によって実現される。該方法は、アクションのセットまたはプログラム（例えば、HTML ページに埋め込まれた JavaScript プログラム）を含んでいるメッセージを受信することと、アクションのセットの実行をシミュレーションすることとを含む。リストは、実行されたアクションと、実行されたアクションへのユーザが定義可能な入力とを表すように定義される。次いで、実行されたアクションと、実行されたアクションへのユーザが定義可能な入力のリストとは、許容可能なアクションと入力のリストと比較される。実行リスト内の要素が許容可能なアクションと入力のリストに含まれているとき、メッセージとアクションの含まれていたセットは認可される。

【0014】

本発明は、例示的であり、限定的でないことを意図している添付の図面の図に示されている。図では、同じ参照符号は、同じまたは対応する部分を指すことを意図している。

【0015】

（好ましい実施形態の詳細な説明）

図1Aは、本発明の一実施形態により構成されかつ動作するクライアント／サーバ・データ処理ネットワーク10を示す。データ処理ネットワーク10は、1つまたは複数のホスト／サーバ・コンピュータと連結され、かつ通信している、パーソナル・コンピュータ、ワーク・ステーション、携帯式および／または手持ち式装置など、複数のクライアント・システムを含む。図示を明瞭にするために、複数のクライアントは、クライアント・システム12によって表し、1つまたは複数のサーバは、サーバ14によって表している。クライアント12とサーバ14は、例えばインターネットのワールド・ワイド・ウェブの部分（「ウェブ」）、イントラネット、エキストラネット、または他の個人的なネットワークなど、通信ネットワーク16に有線接続または無線接続を介して結合された、遠隔装置および／または局所装置とすることが可能であることを理解されたい。

【0016】

本発明によれば、認可プロキシ・システム18は、クライアント12とサーバ

14の間で結合されており、クライアント12とサーバ14の間でセキュリティ・ポリシ・プロトコルを強化する。例えば、認可プロキシ・システム18は、認可されたアクション（以下で定義）のみが、クライアント12とサーバ14との間で送信された要求、メッセージ、データ、情報内容、アプリケーション、および他の情報などの内部において実施されることを保証する。認可プロキシ・システム18は、クライアント12とサーバ14との間で送信された要求、メッセージ、データ、情報内容、およびアプリケーションの内部にあるコマンド、フィールド、ユーザ選択可能入力オプション、HTTP要求など（例えば、「要求されたアクション」）の実行をシミュレーションし、要求されたアクションが、許容可能なアクション（例えば、「認可されたアクション」）のセット内において定義されることを保証する。許容可能なアクションのセット内に存在しないあらゆるアクションは、アクションの標的（例えば、サーバ14またはクライアント12）に到達し、おそらくはそれを破壊する前に、認可プロキシ18によって拒否される。

【0017】

認可プロキシの実装戦略を変更することは、本発明の範囲内にあることを理解されたい。例えば、図1Aは、サーバ14とは分離した別個のネットワーク10のハードウェア構成要素18として認可プロキシを示す。図1Bでは、認可プロキシは、サーバ20上で実行するアプリケーション・プログラミング論理（「プラグイン」論理26）として実装されている。また、サーバ20は、例えばデータ・ストア28に含まれている、またはウェブ・ページ30の上に含まれている、サーバ20にあるアプリケーション・プログラム、情報内容、およびデータを、要求のあり次第クライアント12に提供するためのプラグイン論理22および24を含む。本発明によれば、認可プラグイン論理26は、送信する前に、クライアント12に提供されるプログラム、内容、およびデータを確認するために、サーバ20の上で実行される。

【0018】

別法として、図1Cは、ネットワーク10'上のルータまたはハブ42に結合されたスニファ装置40内において侵入検出システムとして動作する認可プロキ

シを示す。一般に知られているように、ハブ42は、ネットワーク10' 内において通信を向ける。図1Cに示したように、ハブ42は、ネットワーク10' 上の直接通信から、ウェブ・サーバ44を隔離する。スニファ40は、ウェブ・サーバ40を標的にした送信を検出し、遮断する。スニファ40は、遮断した送信を評価し、送信内において要求されたアクションを、例えば、記憶装置46内に含まれている認可されたアクションのリストと比較するために、以下で詳述する方法を実行する。受容可能でない場合、スニファ40は、メッセージを変更するか、または、ネットワーク上の他のシステムにメッセージを渡す。

【0019】

本発明の実施形態について、ウェブをベースとするアプリケーションとして特定のアプリケーションを有するように記載しているが、本明細書に記載されているシステムおよび方法が、任意のクライアント／サーバ通信システム、特に、無認可の要求、データ、およびアプリケーションからサーバを保護するのが望ましい通信システム内において適用可能であることは、本発明の範囲内にあることを理解されたい。

【0020】

以下で詳述するように、本発明の認可プロキシは、サーバ・システムの代わりに、クライアント・システム上で実行される論理を確認するために、2つの技術を使用する。第1の技術では、認可プロキシは、クライアント・サイドの論理の実行をシミュレーションし、各可能なコマンド、フィールド、ユーザが選択可能な入力オプション、およびHTTP要求を呼び出すおよび／またはトリガする。その結果、許容可能なブラウザ・アクションの完全なセットが識別され、実際のクライアント・セッションからの後の要求を確認するために使用される。第2の技術では、プロキシは、実際のクライアント・セッション中に、クライアントサイドの論理の実行を追跡する。追跡の結果は、サーバ・リソースに対する要求内において、認可プロキシに送信される。応答して、認可プロキシは、クライアント・サイドの論理の実行をシミュレーションし、シミュレーション中に入力オプションまたは外部データに対する他の要求に遭遇するとき、追跡結果が使用される。成功したシミュレーションは、サーバ・リソースに対するクライアント要求

の承認となり、認可プロキシは、実際の処理のために、要求を適切なサーバに渡す。

【0021】

2つの確認技術は、技術が未知のデータとユーザ介入事象とに関するクライアント論理の問合わせに応答する方法の点で異なっている。これらの技術については、以下で詳述する。

【0022】

本発明の第1の態様では、認可プロキシ（例えば、プロキシ18、「プラグイン」論理26、およびスニファ40）は、クライアントとサーバとの間の送信を評価する方法を呼び出し、サーバから発信されたメッセージ（例えば、JavaScriptオブジェクト）に組み込まれているクライアント・サイドの論理をシミュレーションし、可能な要求されたアクションのリストを抽出する方法を呼び出す。クライアントが、要求を送信する場合、要求されたアクションは、認可されたアクションのリストに対して確認される。アクションが許容可能である場合、送信は、意図した標的の上に渡され、したがって、意図したアプリケーションに矛盾しない要求のみが実施される。

【0023】

図2は、データ処理システムのクライアントとサーバとの間における伝送を確認するためのプロセス（例えば、前述した評価プロセス、シミュレートするプロセス、および抽出プロセス）を示す流れ図である。例えば、図2は、ウェブ・サーバからクライアント（例えば、図1のサーバ14およびクライアント12）への伝送（例えば、HTMLウェブ・ページ102）を描いている。ブロック100で、サーバ14が、HTMLウェブ・ページ102をクライアント12に伝送する。伝送は、図2において線104Aおよび104Bで表されている。図1A～1Cおよび図2に示すとおり、クライアント12に対するどの伝送も、それぞれ、認可プロキシ18、26、40によって代行受信される。これにตอบสนองして、認可プロキシは、確認プロセス（その詳細を破線106内に示す）を呼び出す。

【0024】

ブロック108で、評価プロセスが呼び出される。評価プロセスには、例えば

、HTMLページ102を構文解析して、内容およびHTMLタグ、ならびにその中に組み込まれたクライアント側論理（例えば、JavaScriptコード）を識別することが含まれる。HTMLページ102中に存在する構成要素が識別されると、認可プロキシは、ページ102の構成要素の実行をシミュレートして（例えば、シミュレートされたブラウザ環境）、可能なすべての要求された処理を伝送の中で識別することができ、認可された処理のリストに提供できるようにする。

【0025】

シミュレートされたブラウザ環境には、シミュレートされたブラウザのDocument Object Model（「DOM」）およびブラウザ・オブジェクトが再現される、それぞれ、ブロック110および112、JavaScriptランタイム環境が含まれる。JavaScript標準オブジェクトのいくつかは、以下にさらに詳細に説明するとおり、置き換える必要がある。認可プロキシが、シミュレートされた環境内でHTMLページ102の構成要素を実行する。環境内のフックが、あらゆるトリガされたブラウザ処理、例えば、WEBサーバからドキュメントを検索する処理、またはWEBサーバに書式をサブミットする処理を認可プロキシに知らせる。シミュレーションが完了すると、これらの処理は、以下に説明するとおり、クライアントの実際の要求（ブロック120における）に対してマッチされた認可された処理のリストを補足する。

【0026】

前述したとおり、オブジェクトのいくつかおよびそのメソッドは、クライアント・ブラウザ環境を表すようにシミュレートされる必要がある。その第1に来るのは、HTMLドキュメント102から作成されるDOMである。さらに、Navigatorなどのブラウザ・オブジェクトが存在し、このオブジェクトは、Netscapeにおいて、ブラウザ・コンテキストおよびブラウザ・ウィンドウに関する情報を提供する。列挙エンジン（ブロック114における）が、DOM構成要素およびJavaScript構成要素のシミュレーションを調整する。また、時間オブジェクト、ランダム関数などのオブジェクトも、列挙エンジンによってシミュレートされる。これらのオブジェクトすべては、スクリプトがク

ライアントの環境内、例えば、クライアント・ブラウザ122上でそれらにアクセスした場合、スクリプトが獲得するものと整合性を有していなければならない。例えば、DOMのテキスト領域は、ユーザがブラウザ122に入力した値を返さなければならない、ランダム関数は、クライアント・スクリプトがユーザのブラウザ122内で獲得したのと同じ値を返さなければならない、またnavigator.userAgentは、クライアント・ブラウザ122の名前を戻さなければならない。

【0027】

理解されたとおり、ブラウザ・オブジェクトに入力されるデータのいくつかは、エンベロープ・データから推論され、例えば、navigator.userAgentは、クライアント12から送信されたHTTPヘッダから獲得することができる（例えば、HTMLページ102のオリジナルの要求の中で）。ただし、いくつかのデータは、クライアント側で辿られる実際のシナリオに依存する。JavaScript中に存在するイベント・ハンドラ（例えば、ユーザの行動に応答して実行されるコード）にさらなる複雑さが導入される。JavaScriptのHTMLスクリプト・タグは、ロードされると実行されるが、ある種のコード（例えば、イベント・ハンドラ）は、ユーザの介入があったときにだけ実行される。例えば、HTML言語の入力コントロールの多くに関するonclickイベント・ハンドラが存在する。対応するイベント・ハンドラは、ユーザがコントロールを選択した（例えば、「クリックした」）ときだけ実行される。

【0028】

列挙エンジン（ブロック114）が、カバレッジ・メソッドを行う。例えば、エンジンは、HTMLページ102中のすべてのイベントをトリガすることにより、またユーザによる可能な様々な入力に対する複数のシミュレートされた実行を行うことにより、ブラウザ122による可能なすべての処理をカバーするものと想定する。理解されたとおり、この環境の実行時間は、多くの入力コントロールに依存するスクリプトの場合、指数関数的に増大する。また、この環境内でランダム関数を扱うのが困難である可能性がある。シミュレートされた実行は、その実行がユーザ入力を要求するまで進行する。要求の時点で、様々な可能な入力

値でさらなる実行を記録し、シミュレートするのにユーザの行動が必要とされる。シミュレーション・メソッドのこの態様は、図3を参照して以下により詳細に述べる。

【0029】

シミュレーションが完了すると、サーバから発信されたHTMLページ（および関連するクライアント側論理）と整合性を有する可能なすべてのブラウザ処理のリストが提供される。これらの可能な処理は、ブロック118で集約され、「正規の処理」として識別される。正規の処理は、認可プロキシによって利用されて、クライアント・ブラウザ122におけるHTMLページ102の特定の実行から受信される要求の処理を確認する。ブロック120で、クライアントの要求の処理が認可プロキシに戻され、認可プロキシによってHTMLページ102のシミュレーションから生成された正規の処理のリスト118と比較される。したがって、認可プロキシは、正規の処理のリスト118中にその要求および有効なユーザ入力が存在するか、存在しないかに応じてクライアントの要求を受け入れるか、または拒否する（例えば、対応する正規の処理が認可プロキシによって識別されなかった場合、要求の処理は拒否される）。正規の処理のリスト118は、クライアント・ブラウザ122からの要求の処理の受信における遅延に対応するように記憶するのが可能である（例えば、データ・ストア30（図1B）または46（図1C）に）ことを理解されたい。

【0030】

図3を参照して、以下に、HTMLページ102のシミュレートされた実行のなかでユーザ入力の要求および複数の可能な入力された値を扱うオプションを説明する。前述したとおり、ブロック150で、認可プロキシが、HTMLページ102中に含まれるブラウザ・コマンドおよびクライアント論理の実行をシミュレートする。シミュレートされた実行は、入力コントロールが現れるまで（ブロック155で）続くか、または他のユーザ入力の要求が行われる（ブロック165で）。ブロック155で、例えば、<TEXT>、<PASSWORD>&<TEXTAREA>のHTMLタグなどのフリー・テキスト入力コマンドが、HTMLページ102中で検出される。フリー・テキスト入力コマンドが現れた場

合、コントロールは、ブロック160に進み、クライアントから受信した入力を表す固有プレース・ホルダが割り当てられる。ブロック160で割り当てられるプレース・ホルダは、例えば、ユーザの行動に応答してフリー・テキスト入力コマンドから生成された入力として生成されたURL内で後に認識されるフィールドである。この後の段階で、認可プロキシは、受信したクライアント要求とのパターン照合を行う（図2のブロック120）。パターン照合は、「安全な」表現だけを許可するように実施する。好ましいパターン照合の技法は、本出願の出願人に共通で譲渡された米国特許出願第09/345920号（弁理士整理番号3269/6）に記載されるHTMLリンク抽出器からもたらされる。プレース・ホルダを含む文字列に基づいて分岐判定（文の場合）を認識するフックが、JavaScript環境の中に組み込まれる。そのような場合、これは、入力がスクリプトの論理進行に影響を与えることを意味するので、実行が無効にされる。システムは、プレース・ホルダが、生成されたURL中に直接に現れることにより、またはプログラムの実行フローに影響を与えることにより間接に、生成されたURLに影響を与える場合、リンクを有効にすることができる。

【0031】

制御は、ブロック160からブロック165に進むか、またはフリー・テキスト入力コマンドが全く現れない場合、ブロック155からブロック165に進む。ブロック165で、認可プロキシが、いくつかの可能な入力値の1つからのユーザによるコマンド要求入力の出現を検出する。そのようなコマンドが現れた場合、コントロールは、ブロック170に進み、現れなければ、コントロールは、ブロック180に進む。ブロック170で、列挙された入力コントロールに対する第1の入手可能な値が割り当てられる。他の可能な正規の入力値も入手可能であるので、制御は、ブロック175に進み、バックトラック・ログ116（図2）中にエントリが行われる。このエントリは、HTMLページ102中の現在の実行の相対位置（例えば、実行における深さ）、ならびに可能な正規のエントリの残りの数を記録する。ログ116は、制御が、前の実行のポイント（深さ）にループバックし、可能な正規の入力値の次の値を選択し、次の正規の入力値で実行を続けるのを可能にすることを理解されたい。ループバックして、HTMLペ

ージ102に対するすべての入力の実行をシミュレートすることにより、可能なすべてのブラウザ・コマンドおよびそれに対するユーザ入力が、前述した可能な正規の処理のリスト118中に収集される。

【0032】

提供された値をログ記録した後、ブロック180で実行が継続する。ブロック180で、シミュレータが、コードの終りを検出する。終りが検出された場合、制御は、可能なバックトラック処理のためにブロック185に進む。終りが現れない場合、制御は、ブロック150にループバックし、前述したとおり、シミュレーションが継続する。ブロック185で、バックトラック・ログ116を評価して、さらなる可能な入力値が、さらなる可能な正規の処理の検出を駆動するかどうか判定される。エントリがバックトラック・ログ116中に残っている場合、深さ変数を利用して、現れた複数の入力コマンドのどれかのところに実行が再配置される。再配置された後、入力コマンドの次の値が割り当てられ、シミュレーションが、相対ロケーションから先にコードの終りまで進む。そのようなループバック実行は、バックトラック・ログ116中の各値が尽きるまで継続される。

【0033】

本発明者は、JavaScript環境におけるバックトラッキングの一実施形態は、バックトラッキング・ポイントまで同一の値で実行を再開することであることを確認した。別の正規の入力がこの時点で提供され、ログ記録される。このプロセスは、列挙されるすべての値が処理されるまで繰り返される。

【0034】

前述したとおり、シミュレーション・プロセス中の可能なすべての入力およびイベントによってトリガされるすべてのブラウザ処理を集約することにより、認可プロキシは、WEBサーバで発信されるスクリプトと整合性を有する、クライアントからの実質的にすべてではないにしても、ほとんどの可能な要求のリストを獲得する。いくつかの実施形態では、このシステムは、以下に説明する追跡実施形態に対する補助として使用されて、より良好なパフォーマンスを得る。

【0035】

以下に、本発明のシミュレーション実施形態の例を説明する。

HTMLページ（例えば、HTMLページ102）が、3つの入力コントロールを含む。

- ・ 2つの国、米国&イスラエルのオプション・リスト（もちろん、完全なリストが可能である）
- ・ 性別、男性&女性のラジオ選択
- ・ ユーザの名前に関するテキスト入力

【0036】

HTML中に組み込まれたJavaScriptが、以下のパターンに従ってURLを構成する。

```
http://site.country.perfectotech.com  
/gender/name.html
```

ここで、countryは、国別により「us」または「il」であり、genderは、「boys」または「girls」という値であり、またnameは、入力テキスト・フィールドである。

【0037】

以下が、HTMLページ・コードである。

```

<HTML>
<HEAD>Test Page</HEAD>
<BODY>
<SCRIPT LANGUAGE=JavaScript>
function openPage ()
{
    var url = "http://site.";

    if (document.form1.country.selectedIndex==0)           [BRANCH A]
        url += "us";
    else if (document.form1.country.selectedIndex==1)
        url += "il";
    else
        url += "intl";

    url += ".perfectotech.com/"

    if (document.form1.gender[0].checked)                  [BRANCH B]
        url += "boys";
    else
        url += "girls";

    url += "/" + document.form1.name.value + ".html";      [ACCESS C]

    var w = window.open (url);
}
</SCRIPT>
<FORM NAME=form1 ACTION=javascript:openPage ()>
Choose your country
<BR>
<SELECT NAME=country>
<OPTION>U.S.</OPTION>
<OPTION>Israel</OPTION>
</SELECT>
<BR>
Your gender is
<BR>
<INPUT TYPE=RADIO NAME=gender VALUE="male">male
<INPUT TYPE=RADIO NAME=gender VALUE="female">female
<BR>
Your name is
<INPUT TYPE=TEXT NAME=name LENGTH=10>

<BR>
<INPUT TYPE=BUTTON VALUE="Get My Page" onClick = "openPage ()">
</FORM>
</BODY>
</HTML>

```

前述したシミュレーション・プロセスは、以下のとおりコードを扱う。

1. ドキュメントの検査により、JavaScriptを実行するイベントは、Get My Pageボタンの上でクリックすることだけであることが与えられる。このイベントがトリガされる。これが、バックトラック・ログ116中に記録され、これがトリガするイベントはこれだけであるという注釈が付けられ、これにより、このエントリが使い果たされる。使い果たしは、後続のステップでより詳細に説明する。
2. ブランチ Aに到達するまでコードが実行される。
3. selectedIndex内で国を表す値が供給され、可能な2つの値、0（米国を表す）および1（イスラエルを表す）が存在する。第1の値が供給され、0の値がブランチ Aで供給されたことが記録される。
4. 実行が、ブランチ Bに進み、Genderラジオ・ボックスのチェックされた値がチェックされる。可能な2つの値、真（boys）および偽（girls）が存在する。真の値が供給されて、バックトラック・ログ116に記録される。
5. 実行が、アクセス Cに到達するまで進み、テキスト・フィールドの値が必要とされる。プレース・ホルダが供給される。このプレース・ホルダは、通常の状態の下では現れる可能性のないUNICODE文字列である。このプレース・ホルダには、<PHname>というマークが付けられる。バックトラック・ログ116にこれをログ記録する必要はない。というのは、この値を対象とするバックトラッキングは、必要とされないからである。<PHname>のタイプが、最大長10のテキストとして記録される。
6. オブジェクトwindowのJavaScript関数openが、要求されたURLを記録する関数にシミュレートされた環境内でフックされる。構成されたURLは、次のようなものである。
`http://site.us.perfectotech.com/boys/<PHname>.html.`
7. ポリシー・エンフォーサが、最大長10の任意のテキストに対して<PHname>をマッチさせるのが可能であるという注釈とともに、この新しい可能な

処理のことを通知される。

8. 実行が再開する。値が次の可能な値、つまり偽で置き換えられた最も深いバックトラッキング・エントリ（ブランチ B）を例外として、同じステップが辿られる。ブランチ Bの可能なすべての値は、使い果たされているので、バックトラック・ログ116中で、使い果たされているというマークが付けられる。

9. したがって、「girls」の値がgenderフィールド内で提供され、生成されるリンクは、`http://site.us.perfectotech.com/girls/<PHname>.html`である。

10. 実行が再開する。今度は、ブランチ Bが最も深い分岐であり、次に許可される値、つまりイスラエルを表す1が提供される。

11. 再びブランチ Bに到達し、今度は、バックトラック・ログ116は存在せず、したがって、（再）更新されたエントリがログ記録され、第1の正規の処理、すなわち、真（boys）が提供される。

12. 実行が、同じパターンで再開し、今度、獲得されるリンクは、次のとおりである。

`http://site.il.perfectotech.com/boys/<PHname>.html`

13. このプロセスは、すべてのバックトラック・ログが尽きるまで反復して（例えば、性別フィールドに対する「girls」の値を提供して、もう一度）続く。したがって、可能なさらなる実行パスは、存在しない。

【0039】

JavaScriptコードを検査する際、要求`http://site.intl.perfectotech.com/...`を生成する可能性がある理論上の実行パスが見られたが、DOMは、0または1以外の国に対するselectedIndexを提供しなかったため、このパスは辿られなかった。これは、どのようにJavaScriptコードとDOMの両方が、許可された要求に影響を与えるかの例である。国に関して可能な値は2つしか存在しなかったため、第3の実行パスは、正規のパスではない。

【0040】

本発明の第2の態様では、認可プロキシ（例えば、プロキシ18、「プラグイン」論理26、およびスニファ40）が、クライアントとサーバとの間の伝送を評価するためのメソッドを呼び出す。第1に、クライアント側論理が、コードに挿入されることによってインストルメント化され、クライアント・システム12上でクライアント側論理の実行を追跡する。クライアント・システム12上でユーザによって実行されると、サーバ・リソースの要求が、実際の実行の結果（追跡結果）とともに認可プロキシにおいて受信される。認可プロキシは、クライアント側論理の実行をシミュレートして、入力オプションまたは外部データの他の要求がシミュレーション中に現れたとき、追跡結果が利用される。成功したシミュレーションは、サーバ・リソースのクライアント要求の承認をもたらし、認可プロキシが、実際の処理のためにその要求を適切なサーバに渡す。例えば、受入れ可能な処理を有する伝送が、意図された目標に伝えられ、これにより、意図されたアプリケーションと整合性のある要求だけが実行される。

【0041】

図4は、データ処理システムのクライアントとサーバとの間の伝送を確認するためのプロセス（例えば、前述した追跡するプロセスおよびシミュレートするプロセス）を示す流れ図である。例えば、図4が、WEBサーバ200からクライアント250への伝送（例えば、HTMLウェブ・ページ202）を描いている。本発明によれば、認可プロキシ（例えば、それぞれ、図1A、1B、1Cのプロキシ18、26、40）が、伝送202を代行受信する。シミュレーション・プロセスに入る前に、認可プロキシは、クライアント・ブラウザ250上で生じる値およびイベントの追跡を可能にするコマンドを受信するための伝送を準備する。ブロック204で、伝送（例えば、HTMLページ202）が構文解析されて、内容およびHTMLタグならびにクライアント側論理（例えば、JavaScriptコード）を識別する。クライアント側論理は、ブロック206に進み、ブラウザ処理（例えば、入力値の要求、および実際の入力値、イベント等）を追跡するためのコードが追加される。次に、変更されたコード、つまりインストルメント化されたコードが、要求された伝送の中（例えば、HTMLページ中202）でクライアント・ブラウザ250に渡される。

【0042】

前述したとおり、インストルメント化されたコードは、ブラウザ処理を追跡して、追跡の結果を認可プロキシに戻す（さらなる処理の要求の中で、またはその要求に加えて）。クライアント・ブラウザ250が、サーバ・リソースを要求したとき、ブラウザ処理のトレース（例えば、クライアント・ブラウザ250上で行われた入力およびイベント）が、評価のために認可プロキシに戻される。この実施形態では、すべての入力を列挙する代りに（図2に概要を述べたシミュレーション・プロセスに関連して説明したとおり）、ブラウザが、その要求とともに、ブラウザ環境内で実際のユーザ・セッション中にスクリプトが獲得したすべての値のトレースを送信する。このトレースは、トレース・フィードにおいて認可プロキシの中で保持される（ブロック212）。

【0043】

追跡の結果が受信されると、認可プロキシが、ブロック210で、オリジナルの伝送（例えば、HTMLページ202）の中のコードおよびDOM構成要素をシミュレートする。図4に示すとおり、シミュレーション・ステップに対する入力は、オリジナルのクライアント側コード（例えば、追跡サポート・コードを有さないクライアント側論理）、DOM構成要素（ブロック208からの）、およびトレース・フィード（ブロック212）からの追跡結果を含む。追跡されたオブジェクトが、シミュレートされた環境内で照会されたとき（ブロック210で）、認可プロキシは、（トレース・フィードを介して）クライアントから受信された追跡された値に関して検査する。また、追跡された値は、オブジェクトの論理上の内容規則に照らしても検査され、例えば、テキスト・フィールド内に許容可能な文字の最大数、または可能な2つの値（真／偽）のどちらかだけでしかないチェックボックス値、他のどの値も不正である。シミュレーションの結果は、ブロック214に渡される受入れ可能な、つまり認可されたブラウザアクションのリストである。ただし、この実施形態では、認可されたブラウザアクションは、第1の確認プロセスに関連して前述したとおり、クライアント・ブラウザにおける特定の実行から決定された値（トレースの中からの入力およびイベント）に基づき、可能なすべてのブラウザ要求に基づくのではない。クライアントアクシ

ョン（ブロック250から渡された）をブロック214で認可されたアクション（ブロック210から渡された）と比較して、特定のクライアント・ブラウザ実行（ブロック250）の要求の1つまたは複数のアクションが認可されるかどうかの判定を行うことができる。

【0044】

理解されるとおり、ブラウザは、デフォルトで追跡を行うこと、および／または追跡の結果を送信することはしない。したがって、ブラウザに送信されるコード（例えば、HTMLドキュメント202）が、シミュレーションに先立って、ブロック206で行われる前述したステップで変更されて（インストルメント化されて）、このコードが、ブラウザ環境内（ブロック250）のブラウザアクションのトレースを作成して戻す。コードに関する例としてのインストルメント化プロセスは、以下を含む。

- ・JavaScriptコードが、JavaScriptアセンブリにコンパイルされる。
- ・アセンブリが、検査され、すべての`get__property`、`set__property`、および関数コールにマークが付けられる
- ・`get__property`命令が、関係のあるプロパティ名に照らして検査される。
- ・関数コールが、追跡された関数値（例えば、ランダム）およびアクション関数（例えば、新しいURLで新しいウィンドウを開く`window.open()`）に照らして検査される。
- ・関係のある命令のそれぞれが、オブジェクトが追跡に関係があるか否かを検査する前に関数コールが挿入される。
- ・`get__property`として、追跡されるオブジェクトの値が、実行トレースに追加される。
- ・新しいURLをロードさせるオブジェクトの`set__property`として、トレースがURLに付加される。
- ・新しいURLをロードする関数コールとして、トレースがURLに付加される。

、ユーザは、コードがインストルメント化されていない場合に見るものと同一の非常に簡単な書式を自らのブラウザ内で見える。

- ・チケット購入の曜日を選択しなければならないことを明記するテキスト
- ・「sunday」というデフォルト値を有する簡単なテキスト・ボックス
- ・要求を送信するボタン

【0049】

ユーザが、「tuesday」を入力して、送信ボタンを選択することによって要求を送信するものと想定する。実際に行われるのは、以下のとおりである。ブラウザ内で、

- ・送信ボタンを選択することにより、my_send関数を呼び出すイベント・ハンドラが起動される。ただし、イベント・ハンドラを起動することは、追跡されるアクションであり、したがって、インストルメント化されたコード中のas_initによって実行トレースに追加される。
- ・JavaScript関数であるmy_sendが呼び出される。この関数は、曜日が、平日の1つの曜日にマッチすることを確認し、ページをマッチするページ、new_page?dayで置き換えるものとされる。
- ・my_send値で、document.forms[0].element.day.valueがアクセスされて、as_propによって追跡される値として識別される。したがって、値「document.forms[0].element.day.value=tuesday」が、トレースに追加される。
- ・コードであるwindow.location.href=「new_page?」+dayが、インストルメント化されたコード中で実行されたとき、as_setpropが、その変数を追跡されるイベント変数として識別する。通常、新しく設定されたURLに対して単一の要求が生成されていることになる。インストルメント化されたコードの中で、生成されたトレースを含む追加の要求がサーバに送信される。

【0050】

この時点で、サーバ内に、要求とトレースの両方がある。

- ・オリジナルのコードがシミュレートされた環境内で実行される。
- ・トレース・フィードが、送信ボタンに関するイベント・ハンドラの起動を識別し、イベント・ハンドラがトリガされる。
- ・イベント・ハンドラが、my__sendを呼び出す
- ・my__sendが、追跡されるオブジェクトである変数「document.forms[0].elements.day.value」にアクセスしようと試みる。
- ・これにより、トレース・フィードが、実行トレースから値「tuesday」を検索する。
- ・トレース・フィードが、サイズ20のテキスト・ボックス内の正規の入力にマッチすることを確認する。
- ・値が、JavaScriptコードに提供される。
- ・JavaScriptコードが、「tuesday」は、実際に平日であることを確認し、window.location.href=「new__page?tuesday」に設定する。
- ・この属性を設定することにより、正しくマッチする実際の要求に対して「new__page?tuesday」のシミュレートされた要求をマッチさせるイベントが生じる。

【0051】

クライアント・システムのユーザ（例えば、ハッカー・オペレーティング・クライアント12）が、サイズ20のテキスト・フィールドに対する正規の入力を構成しない値（例えば、21文字の入力）を提供しようと試みた場合、トレース・フィードは、その値に不正な入力としてマークを付け、その実行を停止することにより、その値をブロックすることになる。ユーザが、不正な要求を提供しようと試みた場合には、シミュレートされた環境処理を実際の要求とマッチさせることに失敗する。

【0052】

本発明を好ましい実施形態で説明し図示してきたが、当分野の技術者には明らかなとおり、本発明の趣旨および範囲を逸脱することなく、多くの変形および変

更を加えることができ、したがって、そのような変形形態および変更形態も本発明の範囲に含まれるものとするので、本発明は、以上に記載した方法または構成の正確な詳細に限定されるべきものではない。

【図面の簡単な説明】

【図 1 A】

本発明の一実施形態により構成されかつ動作する、クライアント／サーバ・データ処理ネットワークのブロック図である。

【図 1 B】

本発明の他の実施形態により構成されかつ動作する、クライアント／サーバ・データ処理ネットワークのブロック図である。

【図 1 C】

本発明のさらに他の実施形態により構成されかつ動作する、クライアント／サーバ・データ処理ネットワークのブロック図である。

【図 2】

本発明の一実施形態によるシミュレーション方法を使用して、クライアントとサーバの間で要求を確認する例示的なプロセスを示すフロー・チャートである。

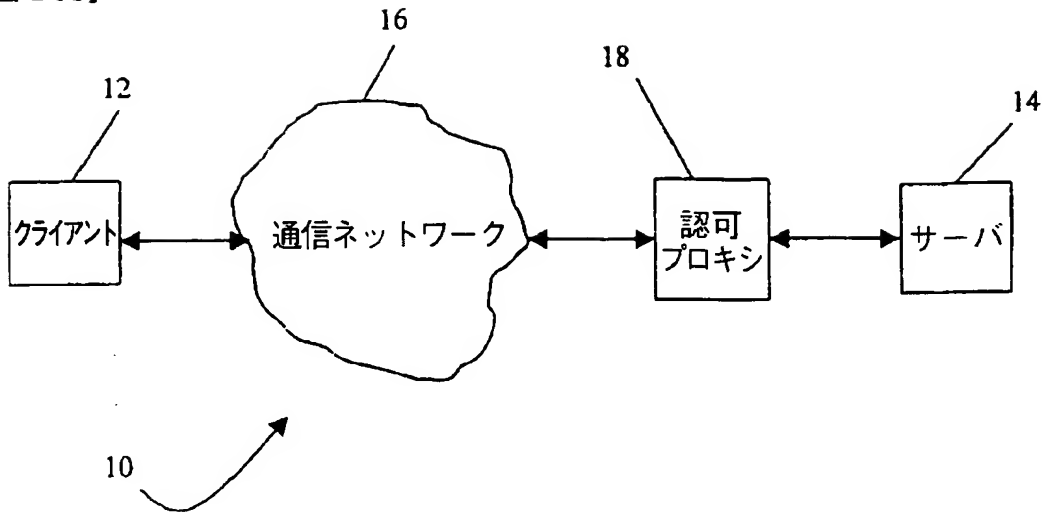
【図 3】

図 2 のシミュレーション方法へのユーザの入力を受け取る例示的なプロセスを示すフロー・チャートである。

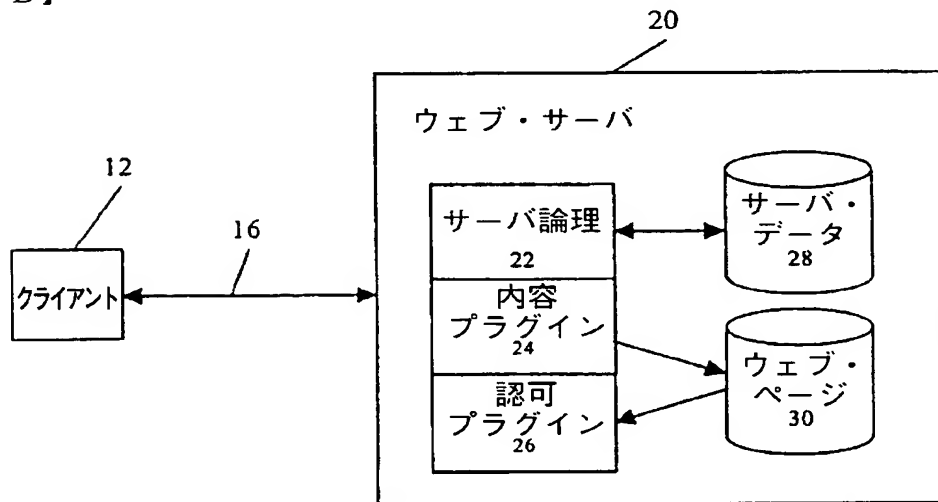
【図 4】

本発明の第 2 実施形態による追跡方法を使用して、クライアントとサーバとの間で要求を確認する例示的なプロセスを示すフロー・チャートである。

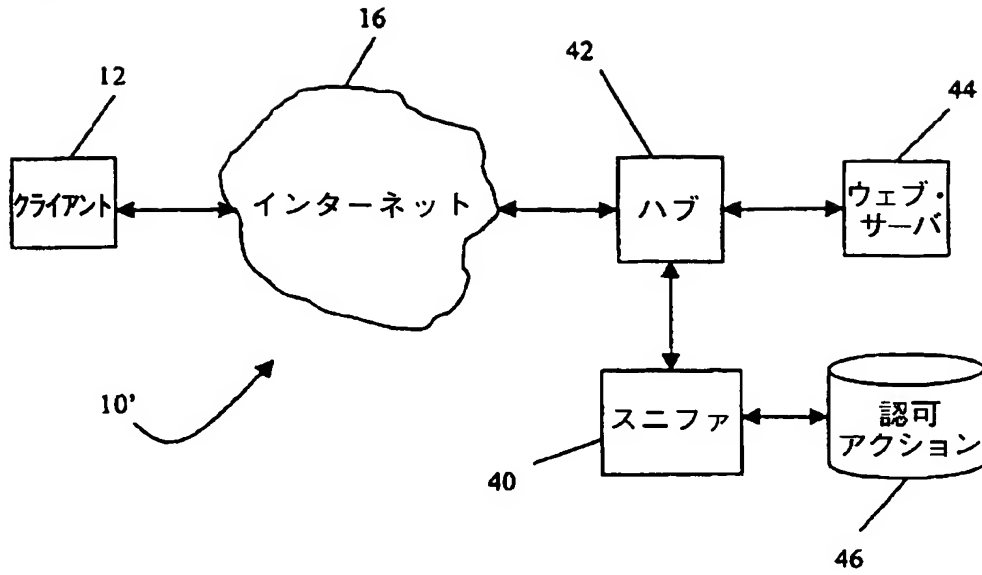
【図1A】



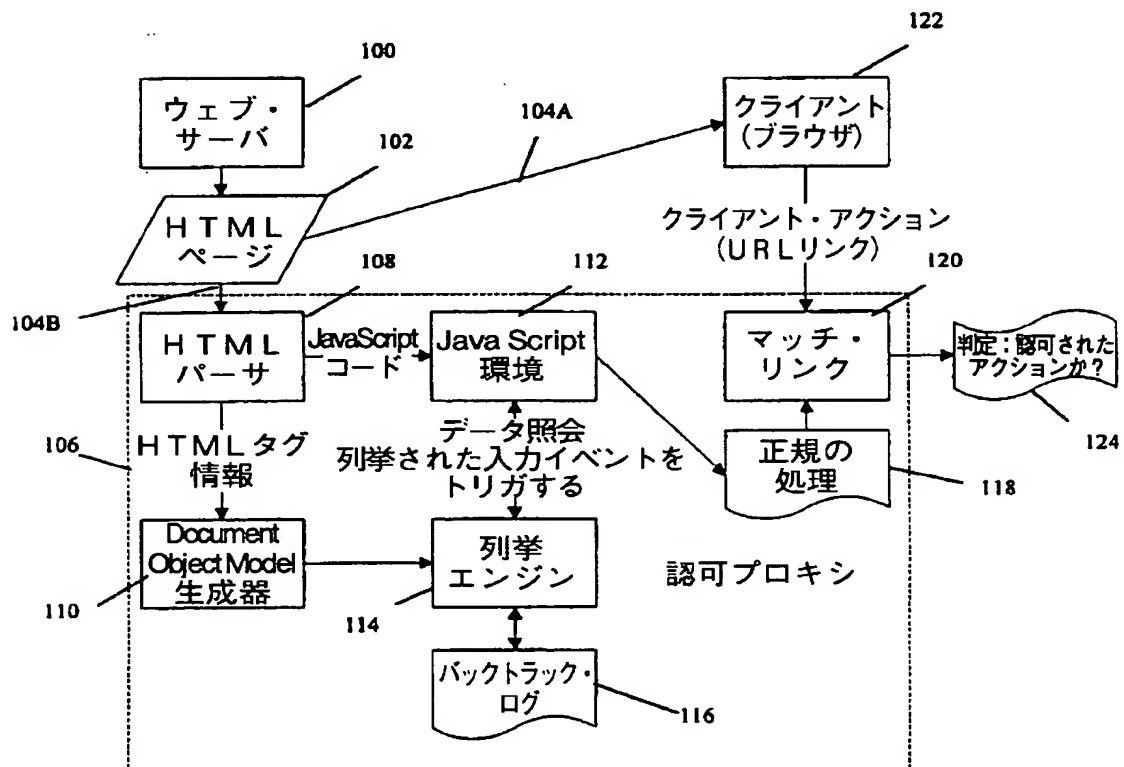
【図1B】



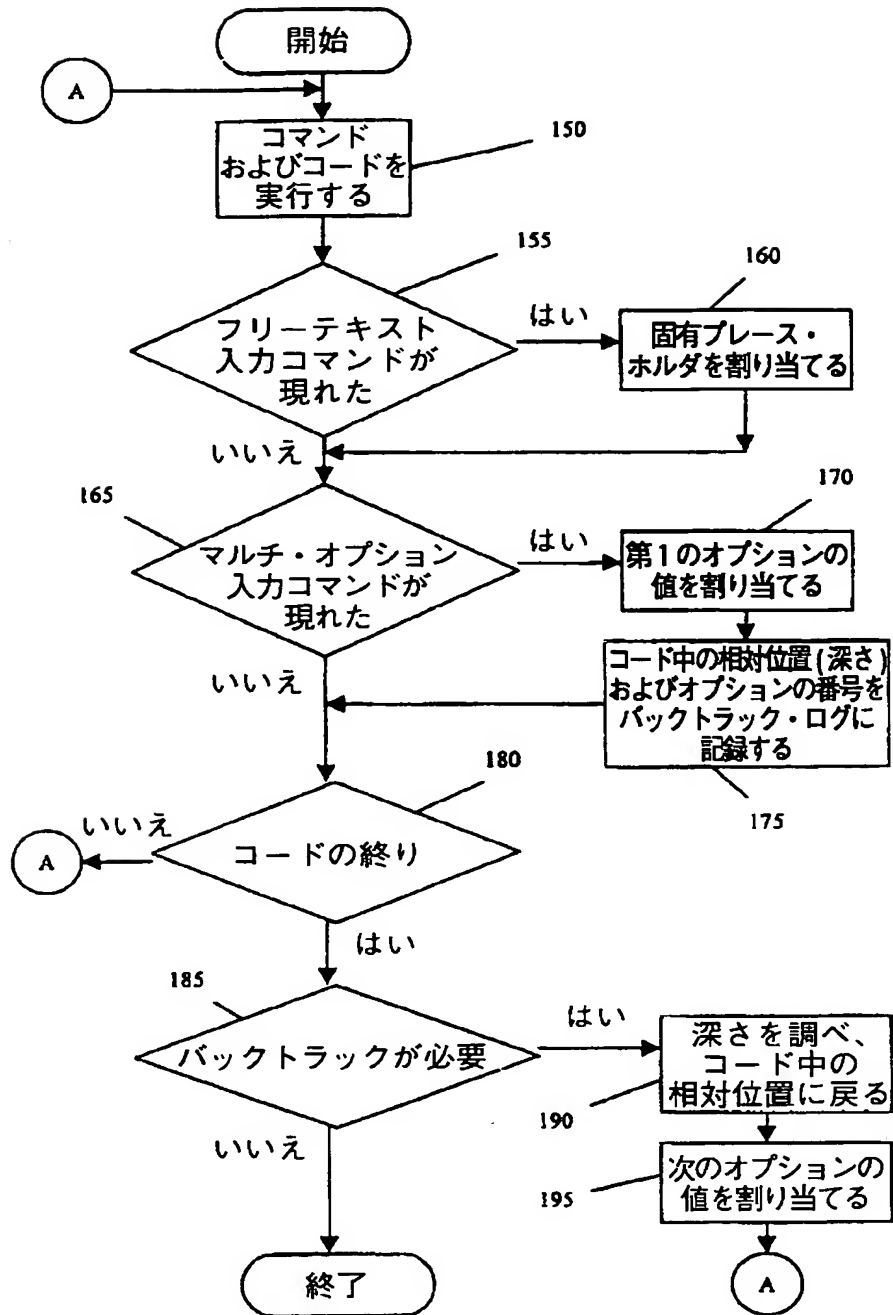
【図1C】



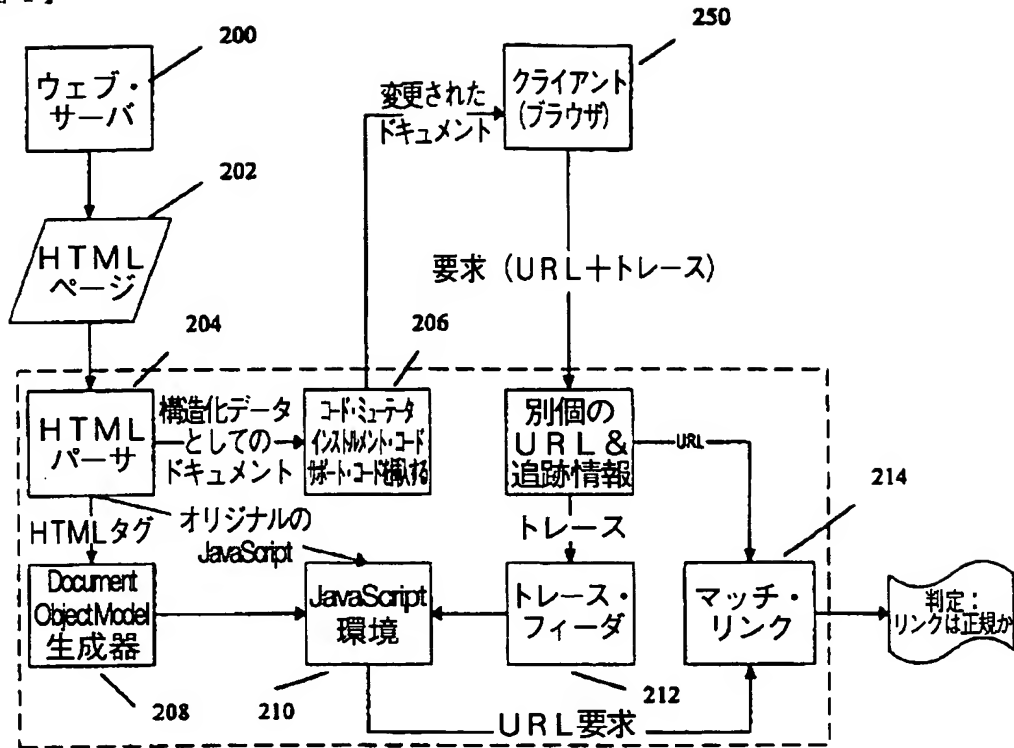
【図2】



【図3】



【図4】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL00/00677

A. CLASSIFICATION OF SUBJECT MATTER		
IPC(7) : H04L 9/00; G06F 9/44, 13/10, 13/12		
US CL : 703/21, 22; 713/153, 154, 164		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
U.S. : 703/21, 22; 713/153, 154, 164		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
EAST 1.2, ACM, IEEE		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim N
X	US 5,623,601 A (VU) 22 April 1997 (22.04.1997), Abstract, 1-7b, Background of the invention, column 3, lines 65 et seq.	1-17
X	US 5,908,469 A (BOLTZ et al) 1 June 1999 (01.06.1999), Abstract, Figures 1A-3, column 2, lines 13 et seq.	1-17
X	US 5,870,544 A (CURTIS) 09 February 1999 (09.02.1999), Abstract, Figures 3-4, Background of the invention, column 4, lines 13 et seq.	1-17
X	US 5,347,578 A (DUXBURY) 13 September 1994 (13.09.1994), Abstract, Figures 1-3, column 1, lines 54 et seq.	1-17
X	US 5,611,048 A (JACOBS et al) 11 March 1997 (11.03.1997), Abstract, Figures 3-9, column 2, lines 65 et seq.	1-17
X	US 5,559,800 A (MOUSSEAU et al) 24 September 1996 (24.09.1996), Abstract, Figures 2-16B, column 5, lines 7 et seq.	1-17
X	SONG W. et al. Design and Implementation of a Security Management System. IEEE 1995, especially page 262, section entitled "Simulator".	1-17
X	PETERSON, K.L. IDA - Intrusion Detection Alert, IEEE 1992, pages 306-311.	1-17
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" documents defining the general state of the art which is not considered to be of particular relevance "E" earlier applications or patents published on or after the international filing date "L" documents which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" documents referred to in oral disclosure, use, exhibition or other means "P" documents published prior to the international filing date but later than the priority date claimed "T" later documents published after the international filing date or prior date and not in conflict with the application but cited to understand principle or theory underlying the invention "X" documents of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" documents of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
09 April 2001 (09.04.2001)		30 APR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. 703-305-3230		Authorized officer KEVIN TESKA <i>Peggy Hamed</i> Telephone No. 703-305-9704

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL00/00677

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of documents, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LIN J. et al. Abstraction-Based Misuse Detection: High Level Specifications and Adaptable Strategies, IEEE 1998, Abstract, Figures 1 and 2, entire document.	1-17
X	SANDHU R.S. et al. Role-Based Access Control: A Multi-Dimensional View, IEEE 1994, Abstract, pages 54-60.	1-17
X	KOGAN B. et al. An Audit Model for Object Oriented Databases, IEEE 1991, pages 90-96.	1-17
X	FREEMAN J. et al. Developing Secure Systems: Issues and Solutions, IEEE 1988, pages 183-189.	1-17
X	BIEBER P. Formal Techniques for an ITSEC-E4 Secure Gateway, IEEE 1996, pages 236-244.	1-17

フロントページの続き

(81) 指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72) 発明者 ラーナン、ギル
イスラエル国 ソラン、ハハダリム ストリート 19

(72) 発明者 レシェフ、エラン
アメリカ合衆国 カリフォルニア、サニー
ヴェイル、 オールド サンフランシスコ
ロード 718

Fターム(参考) 5B085 AE00 BA06 BG07